A.K. Kolodnikov, D.A. Kuznetsova
Ural Federal University named after the first President of Russia B.N. Yeltsin
Yekaterinburg, Russia

INTERNET PRIVACY

Abstract: The article deals with privacy on the Internet and ways to protect it, since the general availability of the Internet and the development of technology have led to the need of reviewing the concepts of privacy and personal data. It also raises questions about spying on users and how to become anonymous online.

Keywords: Internet privacy, personal data, Internet, anonymity.

А.К. Колодников, Д.А. Кузнецова
Уральский федеральный университет имени первого Президента России Б.Н. Ельцина
Екатеринбург, Россия

КОНФИДЕНЦИАЛЬНОСТЬ В ИНТЕРНЕТЕ

Аннотация: В данной статье рассматривается приватность в сети интернет и способы ее защиты, так как общедоступность интернета и развитие технологий привели к необходимости переосмысления понятий частной жизни и персональных данных. Также поднимаются вопросы о слежке за пользователями и о том, как стать анонимным в сети.

Ключевые слова: персональные данные, интернет, приватность, слежка, анонимность.

The Internet is one of the most important phenomena of 21st century. Nowadays people use the Internet for many different purposes. An average internet user produces between 0.32–0.77GB of personal data every day [1]. Personal data is anything that is specific to a person. It covers demographics, location, email address and other identifying factors. It is crucial to keep this data safe.

Some people do not understand why they should worry about privacy and security. Most of them say that they are not criminals and they have nothing to hide. People also believe the Internet is very secure and that their personal information is only available to them, but this is not true [3].

Privacy is when a person can control what data is public and what stays private. Many services on the Internet require users to accept the privacy policy in order to use a service. This is not a user-friendly, privacy-focused model. The ways companies collect and use information are determined by the company's privacy policy. Unfortunately, these are hard-to-read documents that do not always give users a clear idea of how the company uses their data.

Here are the most common threats to online privacy we face daily while surfing the web:

1. Widespread tracking.

Companies like Facebook running the Internet's largest advertising networks use tracking to collect user data [3]. This data is how they implement very specific ad targeting. The smarter the devices people use, the more ways these companies have to collect information.

2. Government surveillance.

Authoritarian governments around the world are some of the worst offenders for tracking their citizens' internet activity. If these governments are able to continue their privacy-invasive tracking, privacy on a global scale may remain a distant reality.

3. Cyber crime.

Identity theft is one of the fastest growing crimes, costing billions of dollars each year. Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain a loan and other benefits in the other person's name. Bank accounts, credit cards, debit cards, social security numbers are the most common targets of this type of crime.

However, there are some ways to avoid these threats. Some of them may be complicated for an average user but there are also easy to install solutions.

1. Disabling cookies.

There is how cookies work: they are little pieces of data stored on a computer. They are used to remember information (like items in an online shopping cart, names, passwords, etc.) about a browsing activity. More secure websites usually have more secure cookies, whereas cookies from other websites lack any encryption at all [2].

It is important to mention that different levels of security can be chosen. Some cookies may be allowed, for example only those from sites that are visited often, some may be completely blocked. Disabling cookies works both on desktop browsers and mobile browsers.

2. Using a private search engine.

Private search engines do not collect and store personal information like big search engines do. These search engines work differently than Google or Yahoo because their business model is completely different. Many of them rely on advertisements within the search results for the revenue, rather than selling their users' information. Some of the good options for privacy focused search engines include DuckDuckGo, Startpage, Search Encrypt, WolframAlpha.

3. Using VPNs.

VPNs, or virtual private networks, allow people to connect to the internet through a remote (or virtual) server. As a result, the data is sent between the device and this server is securely encrypted. Using a VPN gives privacy by hiding internet behavior from both ISP and any other group that may be tracking browsing information. These also work to access blocked websites that otherwise would be impossible to get to due to the internet filters.

4. DNS Leak testing.

While using a VPN, even if an IP address is hidden, it is still possible to give clues about a person's identity via DNS traffic. DNS works to turn a readable web address into an IP address that the computer understands. If the information about this process is leaked, browsing information can be leaked. Luckily, there are tools that will help identify if the connection is leaking DNS data. Here is the most popular service – https://www.dnsleaktest.com/ [2].

5. Using virtual machines.

Using VPNs and encrypted browsers will protect people from the majority of threats. Web browsers are one of the more vulnerable factors for data breaches. However, snooping and data scraping can occur through files such as PDFs. Setting up a virtual machine can help eliminate risks as

virtual machines are similar to having a separate operating system running within one computer.

6. Using a live USB operating system.

Live operating systems can be started on almost any computer from a USB stick or a DVD. Their goal is to maintain privacy and anonymity.

For example, Tails, the live OS preference of Edward Snowden, uses cryptographic tools to encrypt files, emails, and messages. After unplugging the USB there will be no data and no trace of use on the host computer.

All these tools help people to maintain their digital privacy. This is essential because people can use the internet and connected devices without compromising their information. Different persons have different comfort levels when it comes to digital privacy. One person may be comfortable with sharing their name, employer, home address and more on the web, while another may be uncomfortable with any of their information on the web. Digital privacy then, is when the information available online about a given person is within his or her comfort zone.

People are willingly handing over their data to social media and search companies. When a person creates social media profiles or posts to social media, all of that information gets stored on the site's servers. It is not just these companies that could potentially access this information. Social media companies share data with third parties, for example Cambridge Analytica in the case of Facebook.

Due to the fact that data is stored in a way that is linked to personal details, if a hacker accesses it, many people would be at risk. No matter how much users trust Facebook, or Twitter, or Google with storing information, if a third party uses it, hackers could access all information from that third party [2].

Total privacy gives users full control of information shared across the Internet. The key aspect of privacy here is the accessible knowledge about the use of personal data by different companies, because if people are aware of the fact of monitoring, they will have an opportunity to avoid threats and protect themselves from being tracked. Privacy and control of the data gives people the power to be active online without worrying how their personal information might be treated in the future.

REFERENCES

1. Британская Общенациональная общественная телерадиовещательная организация. [Электронный ресурс]. URL: https://www.bbc.co.uk/ (дата обращения 20.01.2019).

2. Новости из мира IT. [Электронный ресурс]. URL: https://www.techopedia.com/ (дата обращения 20.01.2019).

3. Новости интернета. [Электронный ресурс]. URL: https://tjournal.ru. (дата обращения 02.02.2019).

4. Электронная научная библиотека. [Электронный ресурс]. URL: https://cyberleninka.ru. (дата обращения 02.02.2019).